

Lab 2 - Extended Access List

Lab 2: Basic network security—Access-lists (extended)

The physical topology is as shown in Figure 17–2.

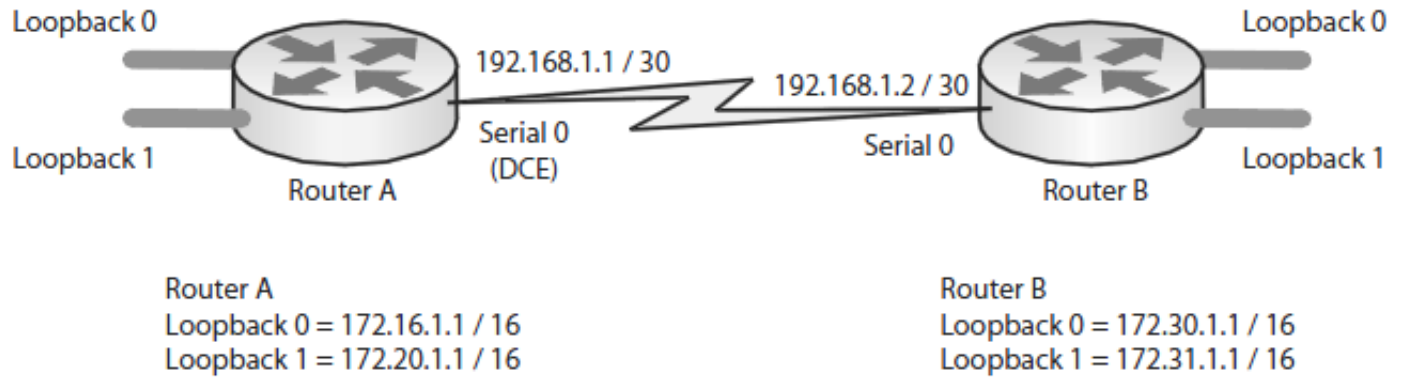


Figure 17–2: Extended access-list

Lab exercise

Your task is to configure the network in Figure 17–2 to allow full connectivity using a default route. Then you will need to configure an access-list to deny telnet connections into router A and Web (HTTP) traffic into router B. Please feel free to try the lab without following the lab walk-through section.

Text written in monospaced type indicates commands that can be entered on the router.

Purpose

Extended access-lists are one of the foundation skills of any competent CCNA. You will be expected to be able to configure one to protect a client's network from certain types of traffic. The number one tip for access-lists is to practice over and over again and also write it out on paper in rough before you configure it (these are two tips I know).

Lab objectives

1. Use the IP addressing scheme depicted in Figure 17–2. The student who is using router A needs to configure a clock rate on interface serial 0: set this to 64000.
2. Set telnet access for the router to use the local login permissions of username "banbury" and the password "ccna".
3. Configure the "enable password" to be "cisco".
4. Configure a default route to allow full connectivity.
5. Configure an access-list to deny any telnet connection from the neighboring router, whilst still allowing all other traffic through.
6. Finally, to test that the access-list is working you will need to telnet to your neighbor's

router.

Lab walk-through

1. To set the IP addresses on an interface, you will need to do the following:

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#interface serial 0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.252
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
RouterA(config-if)#interface loopback 0
RouterA(config-if)#ip address 172.16.1.1 255.255.0.0
RouterA(config-if)#interface loopback 1
RouterA(config-if)#ip address 172.20.1.1 255.255.0.0
RouterA(config-if)# ^ Z
RouterA#
```

Router B:

```
Router#config t
Router(config)#hostname RouterB
RouterB(config)#interface serial 0
RouterB(config-if)#ip address 192.168.1.2 255.255.255.252
RouterB(config-if)#no shutdown
RouterB(config-if)#interface loopback 0
RouterB(config-if)#ip address 172.30.1.1 255.255.0.0
RouterB(config-if)#interface loopback 1
RouterB(config-if)#ip address 172.31.1.1 255.255.0.0
RouterB(config-if)# ^ Z
RouterB#
```

2. To set the clock rate on a serial interface (DCE connection only), you need to use the “clock rate #” command on the serial interface, where # indicates the speed:

```
RouterA(config-if)#clock rate 64000
```

Ping across the serial link now.

3. To set telnet access you need to configure the VTY lines to allow telnet access. To do this type (from configuration mode):

```
RouterA(config)#line vty 0 4 « Enters the VTY line configuration
```

```
RouterA(config-line)#login local « This will use local usernames  
and passwords for telnet access
```

```
RouterA(config-line)#exit « Exit the VTY config mode
```

```
RouterA(config)#username banbury password ccna « Creates username  
and password for telnet access (login local)
```

Router B:

```
RouterB(config)#line vty 0 4
```

```
RouterB(config-line)#login local
```

```
RouterB(config-line)#exit
```

```
RouterB(config)#username banbury password ccna
```

4. To set the “enable password” do the following:

```
RouterA(config)#enable secret cisco « Sets the “enable password”  
(encrypted)
```

Router B:

```
RouterB(config)#enable secret cisco
```

To configure a default route there is one simple step (from configuration mode):

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 serial 0 « For all  
unknown addresses,
```

send the packet out of serial 0

Router B:

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 serial 0
```

5. To configure an access-list, there are two steps: first, specify the networks to permit or deny and second, apply the access-list to an interface:

```
RouterA(config)#access-list 100 deny tcp any any eq 23 « Deny any
```

TCP connection using telnet

```
RouterA(config)#access-list 100 permit ip any any « Permit
```

everything else

```
RouterA(config)#interface serial 0
```

```
RouterA(config-if)#ip access-group 100 in « Assign the access-list
```

to the interface and the direction of traffic to be checked

Router B:

```
RouterB(config)#access-list 100 deny tcp any any eq 80
```

```
RouterB(config)#access-list 100 permit ip any any
```

```
RouterB(config)#interface serial 0
```

```
RouterB(config-if)#ip access-group 100 in
```

6. To test this access-list, you will need to telnet to your neighbor's router. If the access-list is working the connection will be denied:

```
RouterA#telnet 192.168.1.2 80 « Telnet'sing port 80 to test
```

```
Trying 192.168.1.2 ...
```

```
% Destination unreachable; gateway or host down
```

Router B:

```
RouterB#telnet 192.168.1.1
```

```
Trying 192.168.1.1 ...
```

```
% Destination unreachable; gateway or host down
```

7. To make sure the access-list is doing its job, remove the access-list from the serial interface and try the telnet connection again. Router B must have the "ip http server" command added, just so we can test the telnet on port 80.

Router B:

```
RouterB#config t
```

```
RouterB(config)#interface serial 0
```

```
RouterB(config-if)#no ip access-group 100 in « Remove the
```

access-list from the interface on Router B

```
RouterB(config-if)#exit
```

```
RouterB(config)#ip http server « Will permit telnet on port 80
```

Router A:

```
RouterA#telnet 192.168.1.2 80 « Telnet from router A to B
```

```
Trying 192.168.1.2, 80 ... Open
```

```
exit ß Type "exit"
```

```
HTTP/1.0 501 Not Implemented
```

```
Date: Mon, 01 Mar 1993 00:17:40 UTC
```

```
Content-type: text/html
```

```
Expires: Thu, 16 Feb 1989 00:00:00 GMT
```

```
<H1>501 Not Implemented</H1>
```

```
[Connection to 192.168.1.2 closed by foreign host]
```

```
RouterA#
```

Router A:

```
RouterA#config t
```

```
RouterA(config)#interface serial 0
```

```
RouterA(config-if)#no ip access-group 100 in « Remove the  
access-list from the interface on Router A
```

```
RouterA(config-if)#
```

Router B:

```
RouterB#telnet 192.168.1.1 « Telnet from Router B to A
```

```
RouterB#telnet
```

```
02:03:55: %SYS-5-CONFIG_I: Configured from console by  
console192.168.1.1
```

```
Trying 192.168.1.1 ... Open
```

User Access Verification

Username: banbury

Password:

RouterA>

The telnet connection should be successful now because the access-list is no longer in use.

Show runs

RouterA#show run

Building configuration...

Current configuration : 799 bytes

!

version 12.1

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname RouterA

!

enable secret 5 \$1\$jjQo\$YJXxLo.EZm9t6Sq4UYeCv0

!

username banbury password 0 ccna

!

ip subnet-zero

!

interface Loopback0

ip address 172.16.1.1 255.255.0.0

!

interface Loopback1

ip address 172.20.1.1 255.255.0.0

!

interface Serial0

ip address 192.168.1.1 255.255.255.252

ip access-group 100 in

clockrate 64000

```
!  
interface Serial1  
no ip address  
shutdown  
!  
interface Ethernet0  
no ip address  
shutdown  
!  
interface BRI0  
no ip address  
shutdown  
  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 Serial0  
no ip http server  
!  
access-list 100 deny tcp any any eq telnet  
access-list 100 permit ip any any  
!  
line con 0  
line aux 0  
line vty 0 4  
login local  
!  
end
```

```
RouterB#show run  
Building configuration...
```

```
Current configuration : 781 bytes
```

```
!
```

```
version 12.1

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
enable secret 5 $1$HrXN$ThpIDHEZdnCbbeA/Ie67E1
!
username banbury password 0 ccna
!
ip subnet-zero
!
interface Loopback0
 ip address 172.30.1.1 255.255.0.0
!
interface Loopback1
 ip address 172.31.1.1 255.255.0.0
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 ip address 192.168.1.2 255.255.255.252
 ip access-group 100 in
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
```



```
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 Serial0  
no ip http server  
!  
access-list 100 deny tcp any any eq www  
access-list 100 permit ip any any  
!  
line con 0  
line aux 0  
line vty 0 4  
login local  
!  
end
```

RouterB#



© 2006-2011 HowtoNetwork.net All Rights Reserved. Reproduction without permission prohibited.